The ISC Int'l Journal of Information Security
ISeCure

January 2010, Volume 2, Number 1 (pp. 1–2)
http://www.isecure-journal.org

From the Editor-in-Chief

Editorial

On behalf of the Iranian Society of Cryptology (ISC), it is my pleasure to bring you the second volume of ISeCure, the ISC's International Journal of Information Security. ISeCure aims to provide a forum for the publication of high-quality original research results in all areas of information security and cryptology. Currently all accepted peer-reviewed papers are freely available online at the journal website (http://isecure-journal.org).

Following the feedback from our valued audience on the content of some published papers and promoting the journal, two concerns are worth emphasizing. First, as mentioned in the Editorial of the previous issue, there is the possibility of publishing "Comment Papers," in case there are any approved comments on the published papers in ISeCure. On receiving a submission containing comments or corrections, we initiate our review process and, if approved, they are included in the earliest issue. For more information on sending a Comment Paper, please refer to the "Authors' Guide." Second, ISeCure is planning the publication of "Special Issues," either focusing on a narrow topic in Information Security and Cryptology, or the extended version of papers accepted for publication in the proceedings of workshops/symposia dedicated to a specific topic in Information Security and Cryptology. Proposals are welcome to the Editor-in-Chief.

This issue of ISeCure includes four papers. Our sincere appreciation goes to Professor Vincent Rijmen, a member of the journal's International Advisory Board, who accepted to submit his invited paper to ISeCure. This issue starts with Professor Rijmen's invited paper, which presents a survey of the eSTREAM project, sponsored by the EU. The project contributed significantly to the recent increase of activity in the research on secure and efficient stream ciphers. The paper also discusses recent time/memory/data and time/memory/key trade-offs relevant to the generic attacks on stream ciphers.

The second paper focuses on network vulnerability analysis using the concept of Cost- (of implementing a countermeasure) sensitive Attack Graphs (CAGs). There are possibilities of having multiple countermeasures with different weights for preventing a single exploit, or a single countermeasure to prevent multiple exploits. The authors introduce a binary particle swarm optimization algorithm with a time-varying velocity clamping, SwarmCAG-TVVC, in order to find a critical set of countermeasures with minimum weight whose implementation results in no path between the initial nodes and the goal nodes of a given cost-sensitive attack graph. A local search heuristic is used to improve the overall performance of the algorithm. The performance of SwarmCAG-TVVC is compared with a greedy algorithm GreedyCAG and a genetic algorithm GenNAG for minimization analysis of several large-scale cost-sensitive attack graphs and the results are satisfactory.

The third paper proposes a hybrid Evolutionary Fuzzy System which employs an Ant Colony Optimization local searcher to enhance its entire learning process. The final classifier consists of a list of Fuzzy if-then rules for the Intrusion Detection classification problem. Application of the learning approach on a benchmark dataset

ISSN: 2008-2045

indicates better classification accuracy for most of the classes of the intrusion detection. The authors conclude the usage of fuzzy classification rules to produce reliable intrusion detection systems.

The forth paper proposes a context-aware role-based access control model for pervasive computing environments, called iCAP. The model provides dynamic role assignment as well as dynamic permission activation considering context information. This makes the model suitable for deployment in heterogeneous environments with unknown users. The model is implemented regarding a proposed architecture and evaluated based on some common criteria.

Rasool Jalili

Editor-in-Chief,

ISeCure